This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE

IEEE

Membership Publications/Services Standards Conferences Careers/Jobs

IEEE Xplore® RELEASE 1.8

Welcome
United States Patent and Trademark Office

» Se

Help FAQ Terms IEEE Peer Review

Quick Links

Welcome to IEEE Xplore®

- Home
- What Can I Access?
- Log-out

Tables of Contents

- Journals & Magazines
- Conference Proceedings
- Standards

Search

- By Author
- Basic
- Advanced

Member Services

- Join IEEE
- Establish IEEE Web Account
- Access the IEEE Member Digital Library

IEEE Enterprise

- Access the IEEE Enterprise File Cabinet

Print Format

Your search matched **5** of **1071730** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or enter new one in the text box.

intrusion detection <paragraph> game Search

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

1 **A game theoretic approach to decision and analysis in network intr detection**
Alpcan, T.; Basar, T.;
Decision and Control, 2003. Proceedings. 42nd IEEE Conference on , Volume: 3 , 9-12 Dec. 2003
Pages:2595 - 2600 Vol.3

[Abstract] [PDF Full-Text (524 KB)] **IEEE CNF**

2 **ICON 2003. The 11th IEEE International Conference on Networks (I Cat. No.03EX671)**

Networks, 2003. ICON2003. The 11th IEEE International Conference on , 28 1 Oct. 2003
Pages:0_1

[Abstract] [PDF Full-Text (372 KB)] **IEEE CNF**

3 **Detecting network intrusions via sampling: a game theoretic appro**
Murali Kodialam; Lakshman, T.V.;
INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Comput Communications Societies. IEEE , Volume: 3 , 30 March-3 April 2003
Pages:1880 - 1889 vol.3

[Abstract] [PDF Full-Text (310 KB)] **IEEE CNF**

4 **Proceedings of 2002 International Conference on Machine Learning Cybernetics (Cat.No.02EX583)**

Machine Learning and Cybernetics, 2002. Proceedings. 2002 International Conference on , Volume: 2 , 4-5 Nov. 2002
[Abstract] [PDF Full-Text (1409 KB)] **IEEE CNF**

5 **Proceedings of the 2002 International Joint Conference on Neural**

Networks. IJCNN'02 (Cat. No.02CH37290)

Neural Networks, 2002. IJCNN '02. Proceedings of the 2002 International Joir
Conference on , Volume: 2 , 12-17 May 2002
Pages:i - xlviii

[Abstract] [PDF Full-Text (1930 KB)] **IEEE CNF**

Copyright © 2004 IEEE — All rights reserved

Your search matched **0** of **1071730** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or enter new one in the text box.

network attack <and> game Search

☐ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

Results:
No documents matched your query.

Copyright © 2004 IEEE — All rights reserved

ACM PORTAL
US Patent & Trademark Office
Subscribe (Full Service) Register (Limited Service, Free) Login
Search: The ACM Digital Library The Guide
+"network attack" +log +game SEARCH
THE ACM DIGITAL LIBRARY
Feedback Report a problem Satisfaction survey

Terms used **network attack log game** Found **2** of **142,346**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 2 of 2

Relevance scale

1 Hacked for the holidays: how an anonymous network attack almost brought One Small Business to its Knees
E. Dibella
March 2002 **netWorker**, Volume 6 Issue 1
Full text available: pdf(385.81 KB) html(33.60 KB) Additional Information: full citation, index terms

2 Protocol scrubbing: network security through transparent flow modification
David Watson, Matthew Smart, G. Robert Malan, Farnam Jahanian
April 2004 **IEEE/ACM Transactions on Networking (TON)**, Volume 12 Issue 2
Full text available: pdf(316.54 KB) Additional Information: full citation, abstract, references, index terms

This paper describes the design and implementation of protocol scrubbers. Protocol scrubbers are transparent, interposed mechanisms for explicitly removing network scans and attacks at various protocol layers. The transport scrubber supports downstream passive network-based intrusion detection systems by converting ambiguous network flows into well-behaved flows that are unequivocally interpreted by all downstream endpoints. The fingerprint scrubber restricts an attacker's ability to determine t ...

Keywords: intrusion detection, network security, protocol scrubber, stack fingerprinting

Results 1 - 2 of 2

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player

PORTAL
US Patent & Trademark Office
Subscribe (Full Service) Register (Limited Service, Free) Login
Search: The ACM Digital Library The Guide
+"intrusion detection" +log +game SEARCH
THE ACM DIGITAL LIBRARY
Feedback Report a problem Satisfaction survey

Terms used **intrusion detection log game** Found **17** of **142,346**

Sort results by relevance
Display results expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 17 of 17

Relevance scale

1 Research track papers: Adversarial classification
Nilesh Dalvi, Pedro Domingos, Mausam, Sumit Sanghai, Deepak Verma
August 2004 **Proceedings of the 2004 ACM SIGKDD international conference on Knowledge discovery and data mining**
Full text available: pdf(215.03 KB) Additional Information: full citation, abstract, references, index terms

Essentially all data mining algorithms assume that the data-generating process is independent of the data miner's activities. However, in many domains, including spam detection, intrusion detection, fraud detection, surveillance and counter-terrorism, this is far from the case: the data is actively manipulated by an adversary seeking to make the classifier produce false negatives. In these domains, the performance of a classifier can degrade rapidly after it is deployed, as the adversary learns ...

Keywords: cost-sensitive learning, game theory, integer linear programming, naive Bayes, spam detection

2 Session 8: Capture of an intruder by mobile agents
Lali Barrière, Paola Flocchini, Pierre Fraigniaud, Nicola Santoro
August 2002 **Proceedings of the fourteenth annual ACM symposium on Parallel algorithms and architectures**
Full text available: pdf(235.82 KB) Additional Information: full citation, abstract, references, index terms

Consider a team of mobile software agents deployed to capture a (possibly hostile) intruder in a network. All agents, including the intruder move along the network links; the intruder could be arbitrarily fast, and aware of the positions of all the agents. The problem is to design the agents' strategy for capturing the intruder. The main efficiency parameter is the size of the team. This is an instance of the well known graph-searching problem whose many variants have been extensively studied in ...

Keywords: graph-searching, mobile agent, network intruder

3 Safely executing untrusted code: Model-carrying code: a practical approach for safe execution of untrusted applications
R. Sekar, V.N. Venkatakrishnan, Samik Basu, Sandeep Bhatkar, Daniel C. DuVarney
October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**
Full text available: pdf(301.30 KB) Additional Information: full citation, abstract, references, citings, index terms

This paper presents a new approach called *model-carrying code* (MCC) for safe execution of untrusted code. At the heart of MCC is the idea that untrusted code comes equipped with a

concise high-level model of its security-relevant behavior. This model helps bridge the gap between high-level security policies and low-level binary code, thereby enabling analyses which would otherwise be impractical. For instance, users can use a fully automated verification procedure to determine if the code ...

Keywords: mobile code security, policy enforcement, sand-boxing, security policies

4 Protocols: Privacy preserving electronic surveillance



Keith B. Frikken, Mikhail J. Atallah

October 2003 **Proceeding of the ACM workshop on Privacy in the electronic society**

Full text available: pdf(150.58 KB) Additional Information: full citation, abstract, references, index terms

Can protocols make privacy concerns no longer clash with security imperatives, by satisfying both? The former seems to preclude the widespread collection and sharing of data about individuals and their activities, whereas the latter (especially national security and law enforcement) seems to require it. This paper gives a step in the direction of satisfying both, by giving protocols that make the data-sharing about individuals and their actions *conditional on these individuals being already o ...*

***Keywords**: privacy, security protocols, surveillance*

5 Internet intrusions: global characteristics and prevalence



Vinod Yegneswaran, Paul Barford, Johannes Ullrich

June 2003 **ACM SIGMETRICS Performance Evaluation Review , Proceedings of the 2003 ACM SIGMETRICS international conference on Measurement and modeling of computer systems**, Volume 31 Issue 1

Full text available: pdf(699.44 KB) Additional Information: full citation, abstract, references, citings, index terms

Network intrusions have been a fact of life in the Internet for many years. However, as is the case with many other types of Internet-wide phenomena, gaining insight into the *global* characteristics of intrusions is challenging. In this paper we address this problem by systematically analyzing a set of firewall logs collected over four months from over 1600 different networks world wide. The first part of our study is a general analysis focused on the issues of distribution, categorization ...

Keywords: internet performance and monitoring, network security, wide area measurement

6 Applications: An analysis of Internet chat systems



Christian Dewes, Arne Wichmann, Anja Feldmann

October 2003 **Proceedings of the 2003 ACM SIGCOMM conference on Internet measurement**

Full text available: pdf(630.55 KB) Additional Information: full citation, references, citings, index terms

Keywords: IRC, chat, network measurements

7 Public-key cryptography and password protocols: the multi-user case



Maurizio Kliban Boyarsky

November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**

Full text available: pdf(1.00 MB) Additional Information: full citation, abstract, references, citings, index terms

The problem of password authentication over an insecure network when the user holds only

a human-memorizable password has received much attention in the literature. The first rigorous treatment was provided by Halevi and Krawczyk, who studied off-line password guessing attacks in the scenario in which the authentication server possesses a pair of private and public keys. In this work we: Show the inadequacy of both the HK formalization and protocol in the ...

8 Protocol scrubbing: network security through transparent flow modification

David Watson, Matthew Smart, G. Robert Malan, Farnam Jahanian

April 2004 **IEEE/ACM Transactions on Networking (TON)**, Volume 12 Issue 2

Full text available: pdf(316.54 KB) Additional Information: full citation, abstract, references, index terms

This paper describes the design and implementation of protocol scrubbers. Protocol scrubbers are transparent, interposed mechanisms for explicitly removing network scans and attacks at various protocol layers. The transport scrubber supports downstream passive network-based intrusion detection systems by converting ambiguous network flows into well-behaved flows that are unequivocally interpreted by all downstream endpoints. The fingerprint scrubber restricts an attacker's ability to determine t ...

Keywords: intrusion detection, network security, protocol scrubber, stack fingerprinting

9 A model for evaluating IT security investments

Huseyin Cavusoglu, Birendra Mishra, Srinivasan Raghunathan

July 2004 **Communications of the ACM**, Volume 47 Issue 7

Full text available: pdf(115.20 KB) html(32.85 KB) Additional Information: full citation, references, index terms

10 LOF: identifying density-based local outliers

Markus M. Breunig, Hans-Peter Kriegel, Raymond T. Ng, Jörg Sander

May 2000 **ACM SIGMOD Record , Proceedings of the 2000 ACM SIGMOD international conference on Management of data**, Volume 29 Issue 2

Full text available: pdf(263.81 KB) Additional Information: full citation, abstract, references, citings, index terms

For many KDD applications, such as detecting criminal activities in E-commerce, finding the rare instances or the outliers, can be more interesting than finding the common patterns. Existing work in outlier detection regards being an outlier as a binary property. In this paper, we contend that for many scenarios, it is more meaningful to assign to each object a *degree* of being an outlier. This degree is called the *local outlier factor* (LOF) of an object. It is *local* in th ...

Keywords: database mining, outlier detection

11 Stalking the wily hacker

Clifford Stoll

May 1988 **Communications of the ACM**, Volume 31 Issue 5

Full text available: pdf(1.60 MB) Additional Information: full citation, abstract, references, citings, index terms

An astronomer-turned-sleuth traces a German trespasser on our military networks, who slipped through operating system security holes and browsed through sensitive databases. Was it espionage?

12 Parsimonious downgrading and decision trees applied to the inference problem

LiWu Chang, Ira S. Moskowitz

January 1998 **Proceedings of the 1998 workshop on New security paradigms**

Full text available: pdf(674.19 KB) Additional Information: full citation, references, citings, index terms

Keywords: data mining, downgrading, inference, rules

13 Paranoid penguin: intrusion detection for the masses

Mick Bauer

July 2001 **Linux Journal**, Volume 2001 Issue 87

Full text available: html(28.18 KB) Additional Information: full citation

14 Improving the adaptability of multi-mode systems via program steering

Lee Lin, Michael D. Ernst

July 2004 **ACM SIGSOFT Software Engineering Notes , Proceedings of the 2004 ACM SIGSOFT international symposium on Software testing and analysis**, Volume 29 Issue 4

Full text available: pdf(195.32 KB) Additional Information: full citation, abstract, references, index terms

A multi-mode software system contains several distinct modes of operation and a controller for deciding when to switch between modes. Even when developers rigorously test a multi-mode system before deployment, they cannot foresee and test for every possible usage scenario. As a result, unexpected situations in which the program fails or underperforms (for example, by choosing a non-optimal mode) may arise. This research aims to mitigate such problems by creating a new mode selector that examines ...

Keywords: adaptability, mode selection, multi-mode systems, program steering

15 Enabling trusted software integrity

Darko Kirovski, Milenko Drinić, Miodrag Potkonjak

October 2002 **Proceedings of the 10th international conference on Architectural support for programming languages and operating systems**, Volume 37 , 30 , 36 Issue 10 , 5 , 5

Full text available: pdf(1.39 MB) Additional Information: full citation, abstract, references, citings

Preventing execution of unauthorized software on a given computer plays a pivotal role in system security. The key problem is that although a program at the beginning of its execution can be verified as authentic, while running, its execution flow can be redirected to externally injected malicious code using, for example, a buffer overflow exploit. Existing techniques address this problem by trying to detect the intrusion at run-time or by formally verifying that the software is not prone to a p ...

16 Communication over wireless LANs: DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots

Maxim Raya, Jean-Pierre Hubaux, Imad Aad

June 2004 **Proceedings of the 2nd international conference on Mobile systems, applications, and services**

Full text available: pdf(301.61 KB) Additional Information: full citation, abstract, references, index terms

The proliferation of hotspots based on IEEE 802.11 wireless LANs brings the promise of seamless Internet access from a large number of public locations. However, as the number of users soars, so does the risk of possible misbehavior; to protect themselves, wireless ISPs already make use of a number of security mechanisms, and require mobile stations to authenticate themselves at the Access Points (APs). However, IEEE 802.11 works properly only if the stations also respect the MAC protocol. We sh ...

Keywords: IEEE 802.11, MAC, WISP, hotspot, misbehavior, wireless LAN



17 Mobile and Cooperative Systems: Information sharing and security in dynamic coalitions

Charles E. Phillips, T.C. Ting, Steven A. Demurjian

June 2002 **Proceedings of the seventh ACM symposium on Access control models and technologies**

Full text available: pdf(1.68 MB) Additional Information: full citation, abstract, references, citings, index terms

Today, information sharing is critical to almost every institution. There is no more critical need for information sharing than during an international crisis, when international coalitions dynamically form. In the event of a crisis, whether it is humanitarian relief, natural disaster, combat operations, or terrorist incidents, international coalitions have an immediate need for information. These coalitions are formed with international cooperation, where each participating country offers whate ...

Keywords: access control, distributed systems, dynamic coalitions, information security

Results 1 - 17 of 17

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.
Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player